Steps to Recover Your Private Encryption Keys

Copy & Past below URL into Browser

Note: <u>The URL addresses shown below are case sensitive</u>

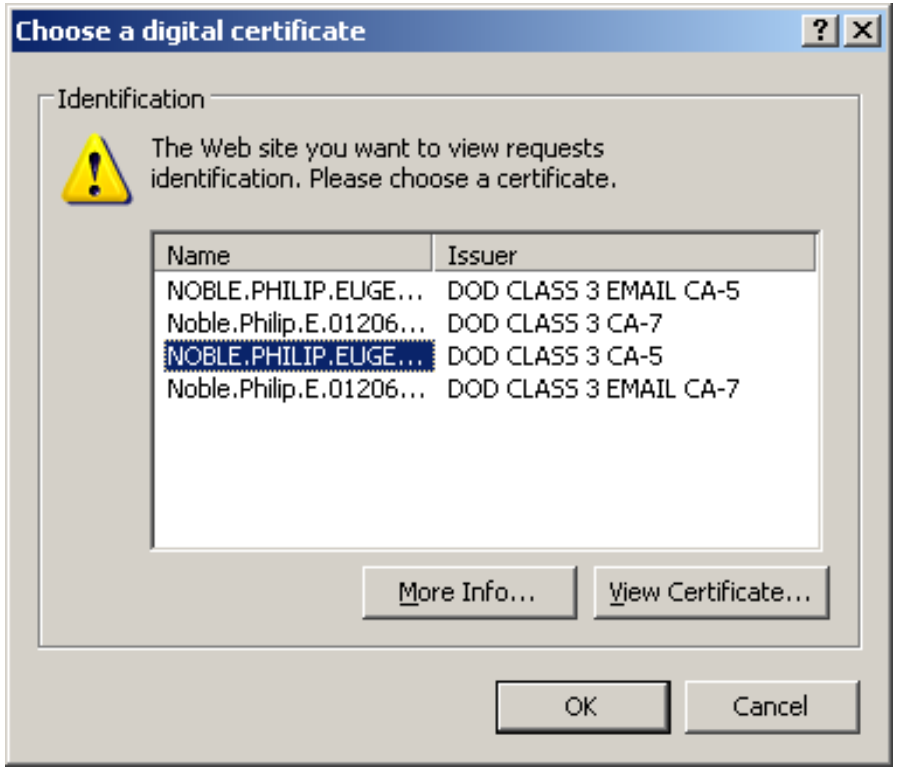
If you are prompted to identify yourself…see next slide

https://
ara-1.c3pki.chamb.disa.mil/ara/Key

Or

https://ara-2.c3pki.dep.disa.mil/ara/Ke

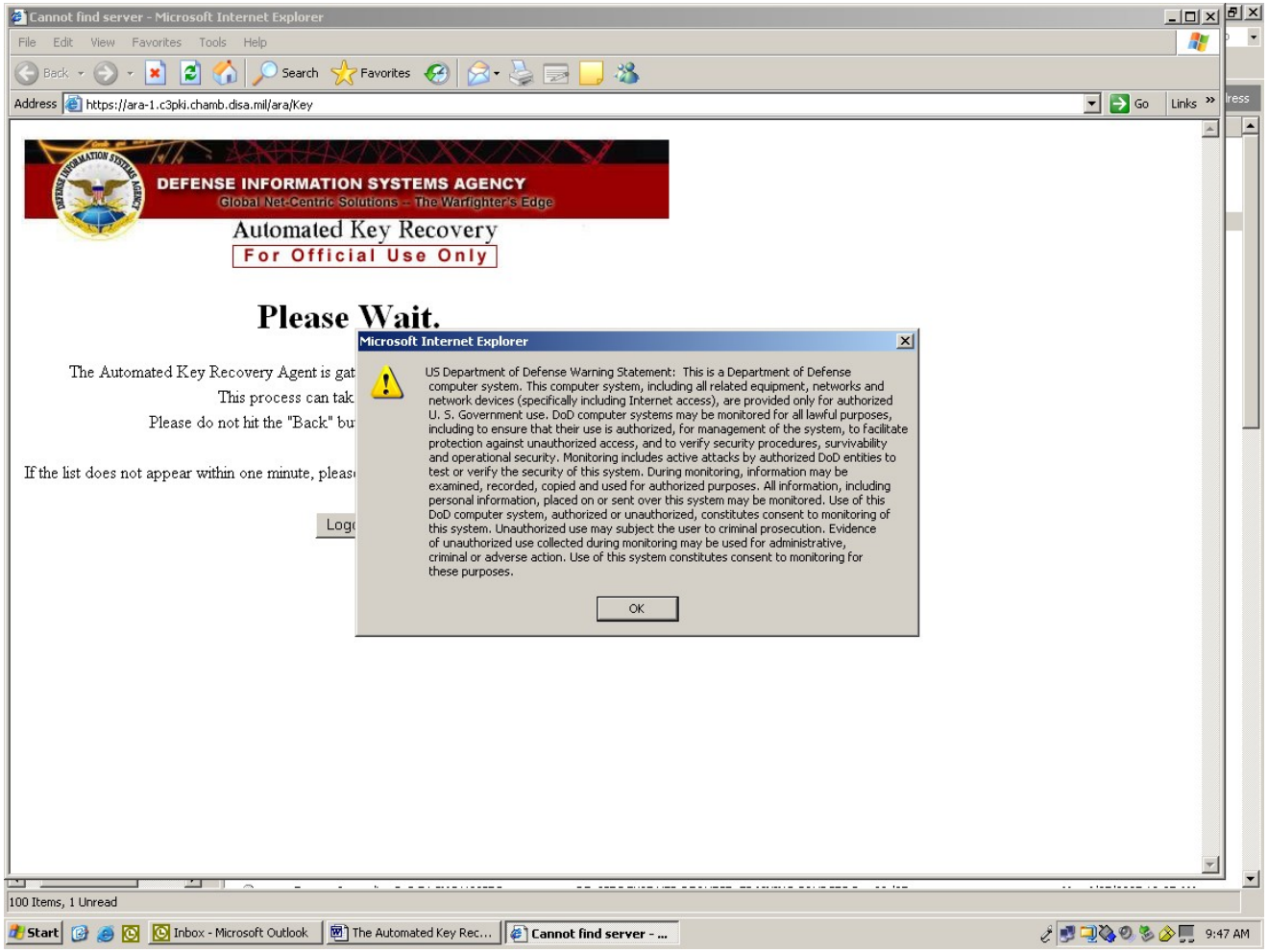
Choose Your CAC Identity Certificate



Highlight <u>your</u> Identification Certificate from your CAC,

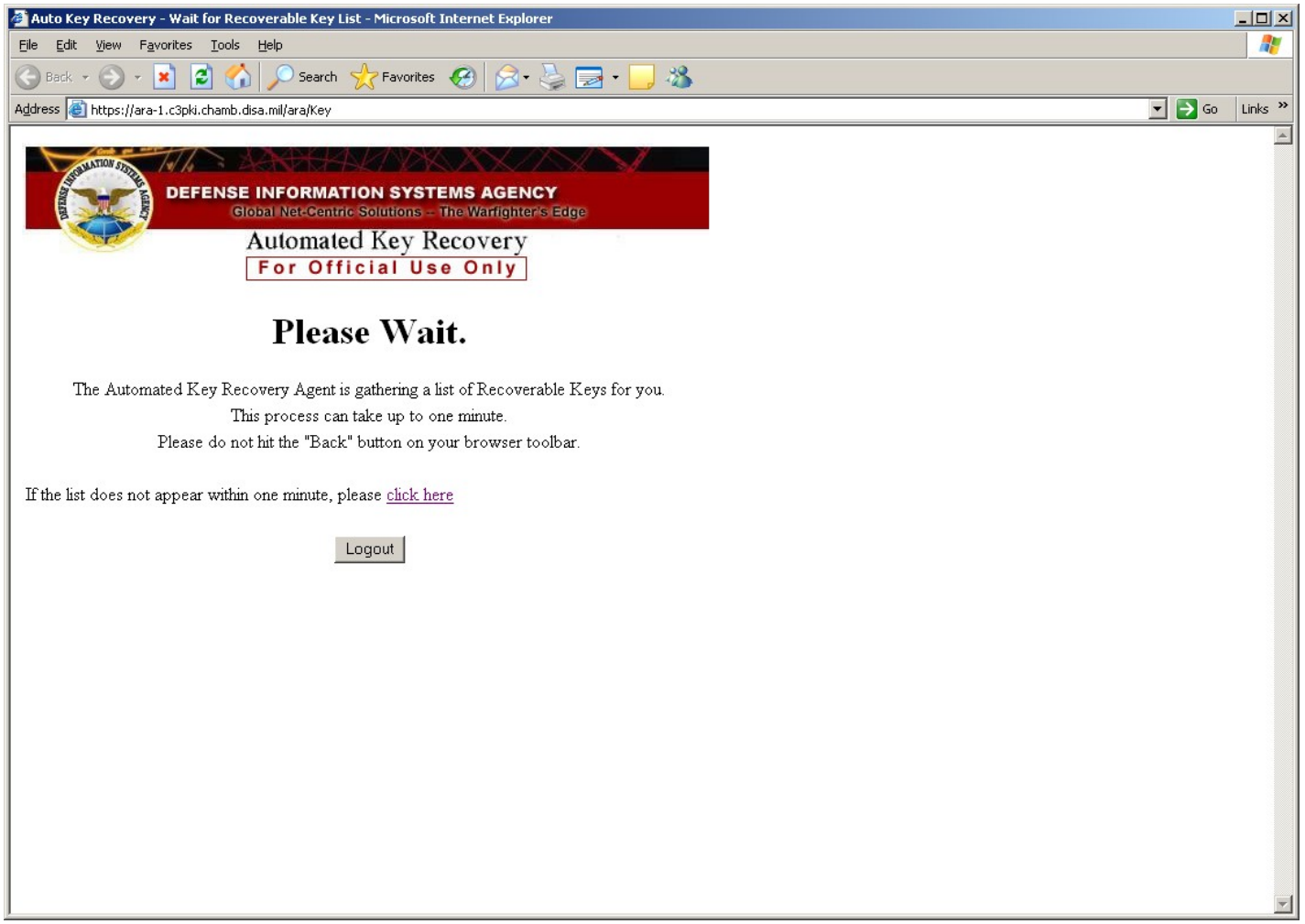
(**NOT** the one that contains the words EMAIL), then click “OK”.

Warning Banner


Cannot find server - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address https://ara-1.c3pki.chamb.disa.mil/ara/Key
Go Links
DEFENSE INFORMATION SYSTEMS AGENCY
Global Net-Centric Solutions - The Warfighter's Edge
Automated Key Recovery
For Official Use Only
Please Wait.
The Automated Key Recovery Agent is gat
This process can tak
Please do not hit the "Back" bu
If the list does not appear within one minute, pleas
Microsoft Internet Explorer
US Department of Defense Warning Statement: This is a Department of Defense computer system. This computer system, including all related equipment, networks and network devices (specifically including Internet access), are provided only for authorized U. S. Government use. DoD computer systems may be monitored for all lawful purposes, including to ensure that their use is authorized, for management of the system, to facilitate protection against unauthorized access, and to verify security procedures, survivability and operational security. Monitoring includes active attacks by authorized DoD entities to test or verify the security of this system. During monitoring, information may be examined, recorded, copied and used for authorized purposes. All information, including personal information, placed on or sent over this system may be monitored. Use of this DoD computer system, authorized or unauthorized, constitutes consent to monitoring of this system. Unauthorized use may subject the user to criminal prosecution. Evidence of unauthorized use collected during monitoring may be used for administrative, criminal or adverse action. Use of this system constitutes consent to monitoring for these purposes.
OK
100 Items, 1 Unread
Start
Inbox - Microsoft Outlook
The Automated Key Rec...
Cannot find server - ...
9:47 AM

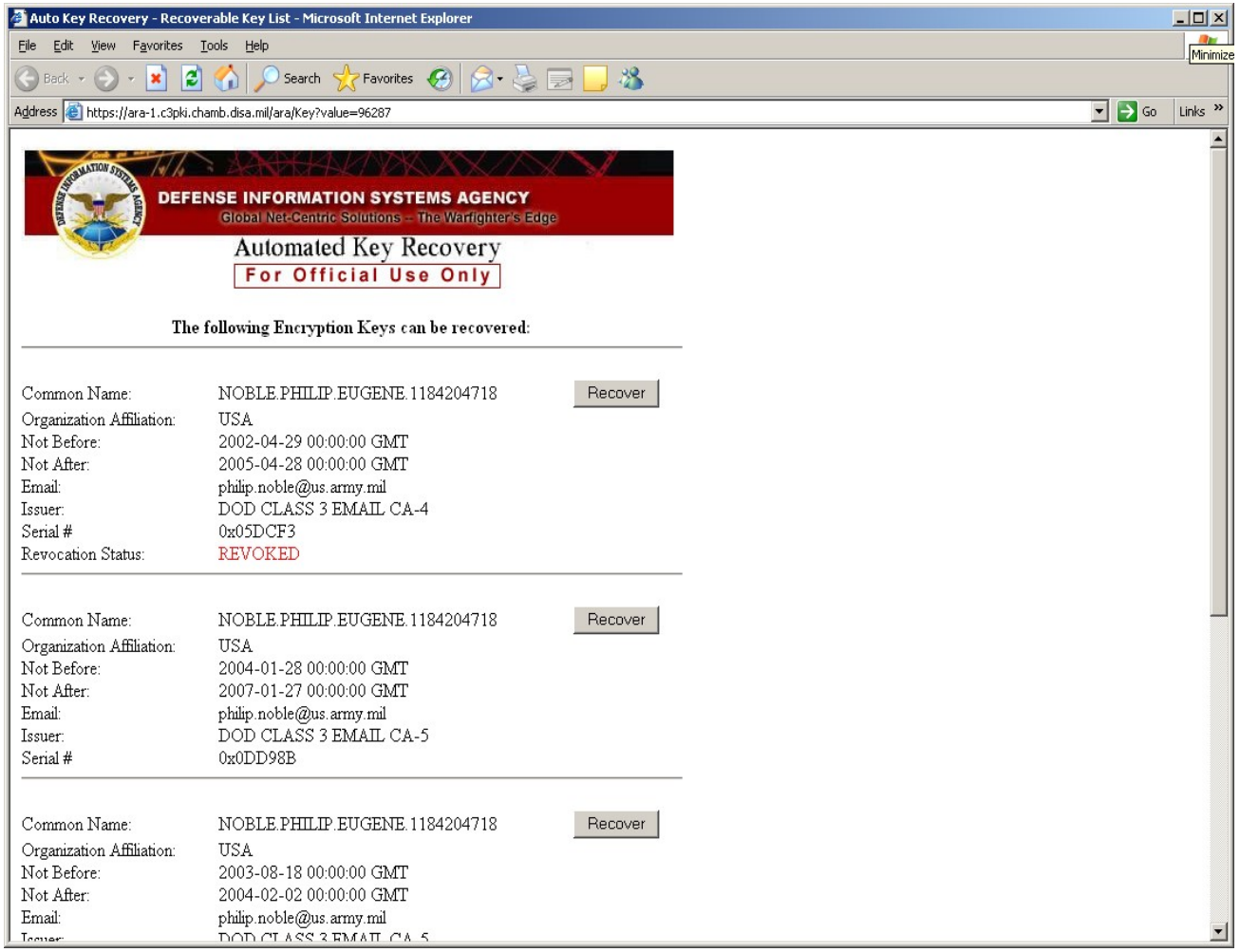
Dismiss the warning by clicking “OK”.

Processing Your Request


Auto Key Recovery - Wait for Recoverable Key List - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address https://ara-1.c3pki.chamb.disa.mil/ara/Key
Go Links
DEFENSE INFORMATION SYSTEMS AGENCY
Global Net-Centric Solutions -- The Warfighter's Edge
Automated Key Recovery
For Official Use Only
Please Wait.
The Automated Key Recovery Agent is gathering a list of Recoverable Keys for you.
This process can take up to one minute.
Please do not hit the "Back" button on your browser toolbar.
If the list does not appear within one minute, please click here
Logout

The Automated Key Recovery Agent will compile a list of Recoverable Keys. Please Wait…

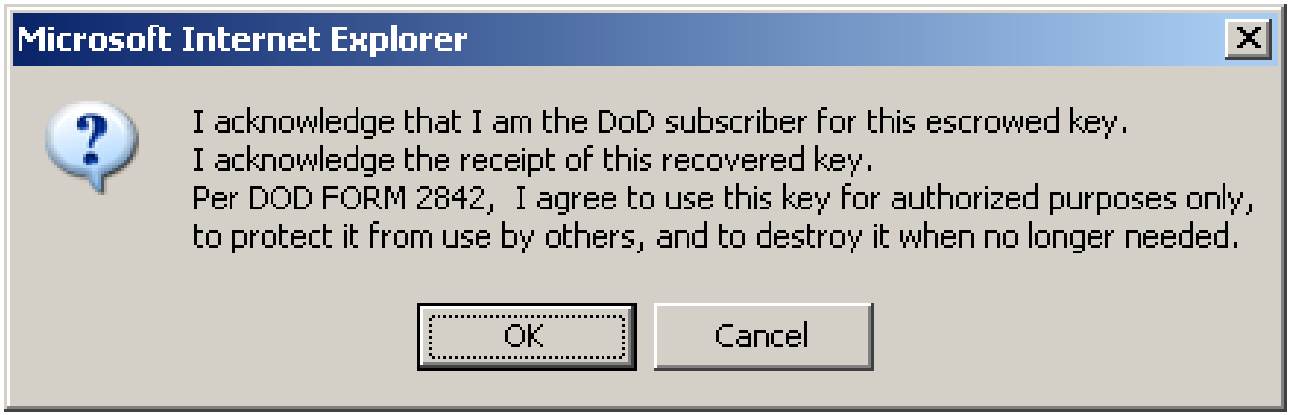
Key Selection



Browse through the list and locate the appropriate key you want to recover.

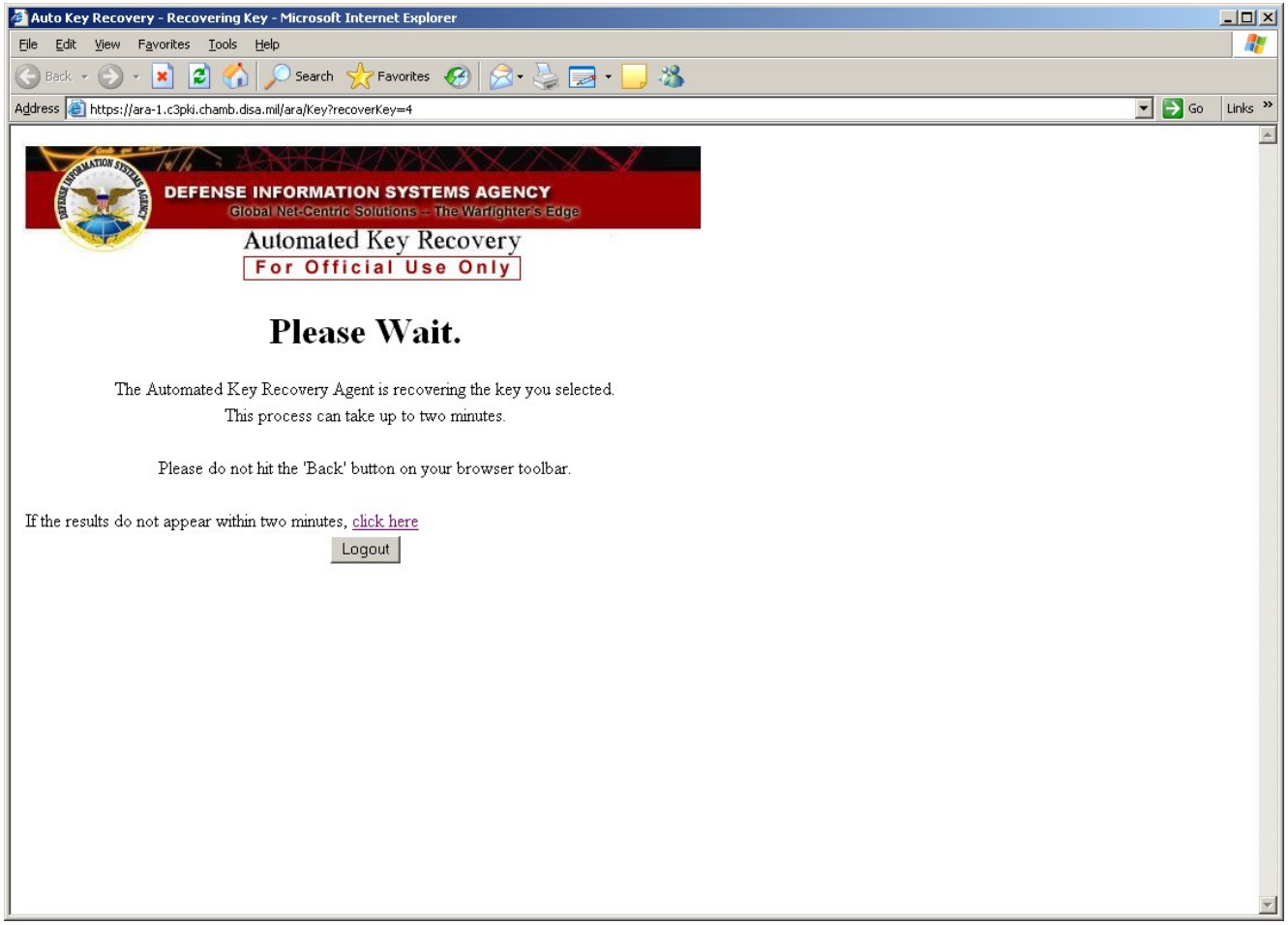
When located, click the adjacent associated “Recover” button.

Acknowledgement of DoD Subscriber


Microsoft Internet Explorer
I acknowledge that I am the DoD subscriber for this escrowed key.
I acknowledge the receipt of this recovered key.
Per DOD FORM 2842, I agree to use this key for authorized purposes only,
to protect it from use by others, and to destroy it when no longer needed.
OK
Cancel

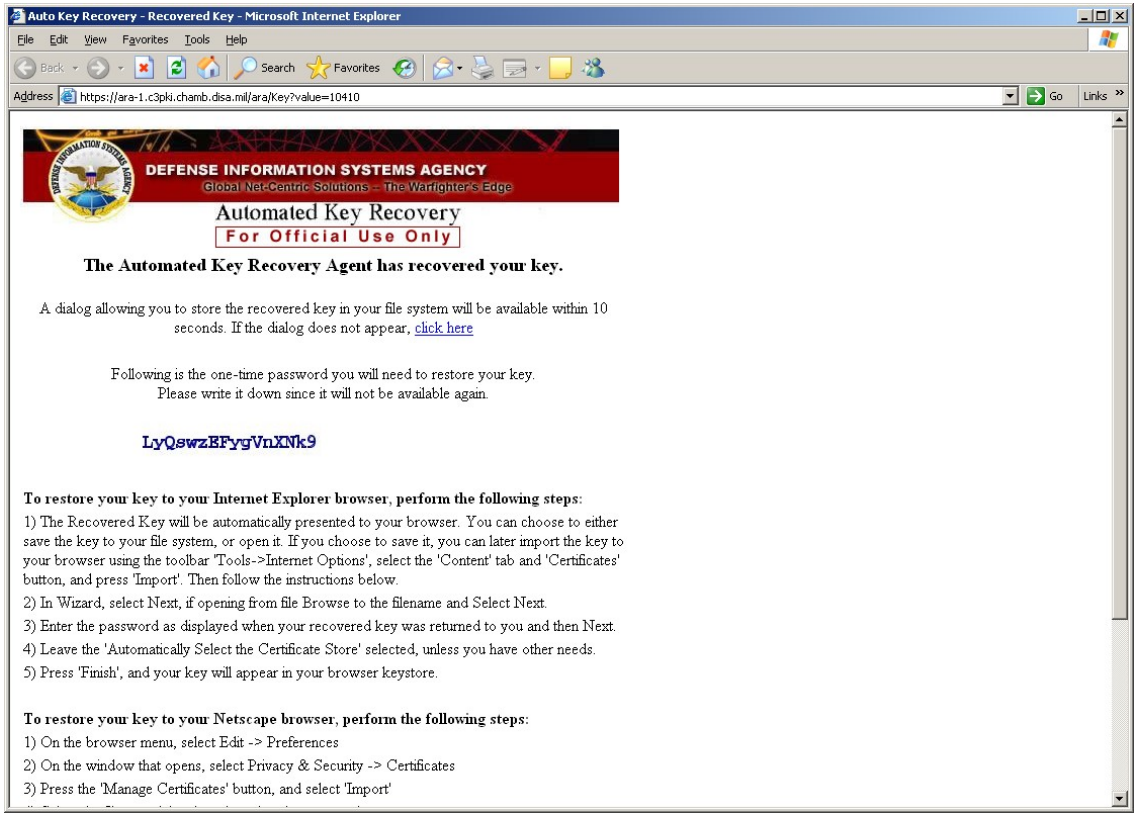
Select “OK”.

Processing Request


Auto Key Recovery - Recovering Key - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address https://ara-1.c3pki.chamb.disa.mil/ara/Key?recoverKey=4
Go Links
DEFENSE INFORMATION SYSTEMS AGENCY
Global Net-Centric Solutions -- The Warfighter's Edge
Automated Key Recovery
For Official Use Only
Please Wait.
The Automated Key Recovery Agent is recovering the key you selected.
This process can take up to two minutes.
Please do not hit the 'Back' button on your browser toolbar.
If the results do not appear within two minutes, click here
Logout

The Automated Key Recovery Agent is processing your request. Please Wait…

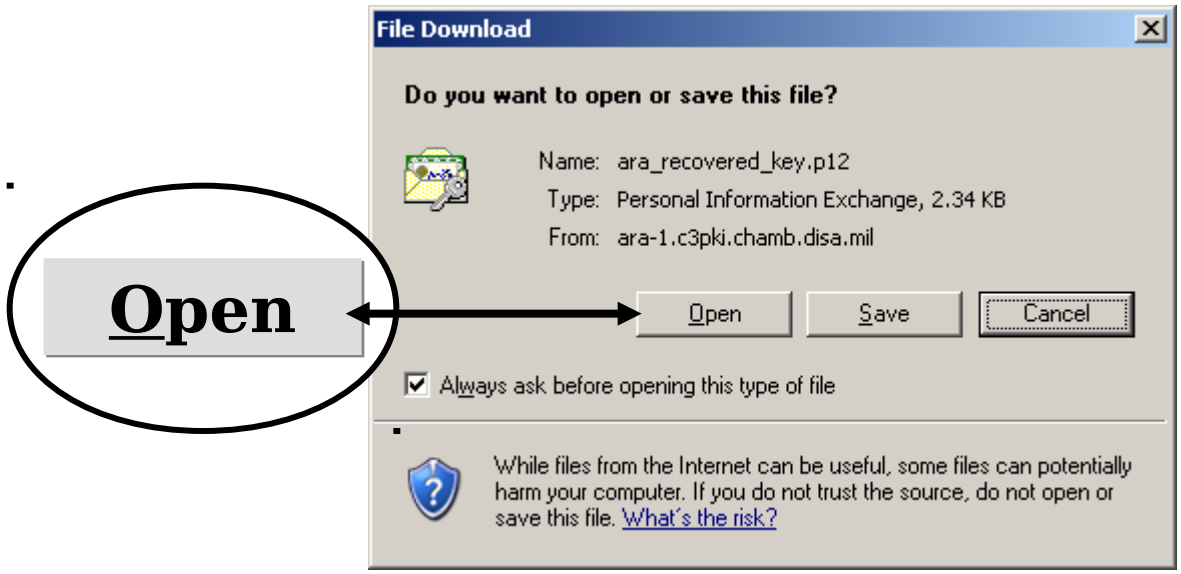
One-time PIN


Auto Key Recovery - Recovered Key - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address https://ara-1.c3pki.chamb.disa.mil/ara/Key?value=10410
Go Links
DEFENSE INFORMATION SYSTEMS AGENCY
Global Net-Centric Solutions -- The Warfighter's Edge
Automated Key Recovery
For Official Use Only
The Automated Key Recovery Agent has recovered your key.
A dialog allowing you to store the recovered key in your file system will be available within 10 seconds. If the dialog does not appear, click here
Following is the one-time password you will need to restore your key.
Please write it down since it will not be available again.
LyQswzEFygVnXNk9
To restore your key to your Internet Explorer browser, perform the following steps:
1) The Recovered Key will be automatically presented to your browser. You can choose to either save the key to your file system, or open it. If you choose to save it, you can later import the key to your browser using the toolbar 'Tools->Internet Options', select the 'Content' tab and 'Certificates' button, and press 'Import'. Then follow the instructions below.
2) In Wizard, select Next, if opening from file Browse to the filename and Select Next.
3) Enter the password as displayed when your recovered key was returned to you and then Next.
4) Leave the 'Automatically Select the Certificate Store' selected, unless you have other needs.
5) Press 'Finish', and your key will appear in your browser keystore.
To restore your key to your Netscape browser, perform the following steps:
1) On the browser menu, select Edit -> Preferences
2) On the window that opens, select Privacy & Security -> Certificates
3) Press the 'Manage Certificates' button, and select 'Import'

You will see a link to download the certificate you chose and a one-time PIN to restore your Private Encryption Key.

Click on the DOWNLOAD link and you should see next slide

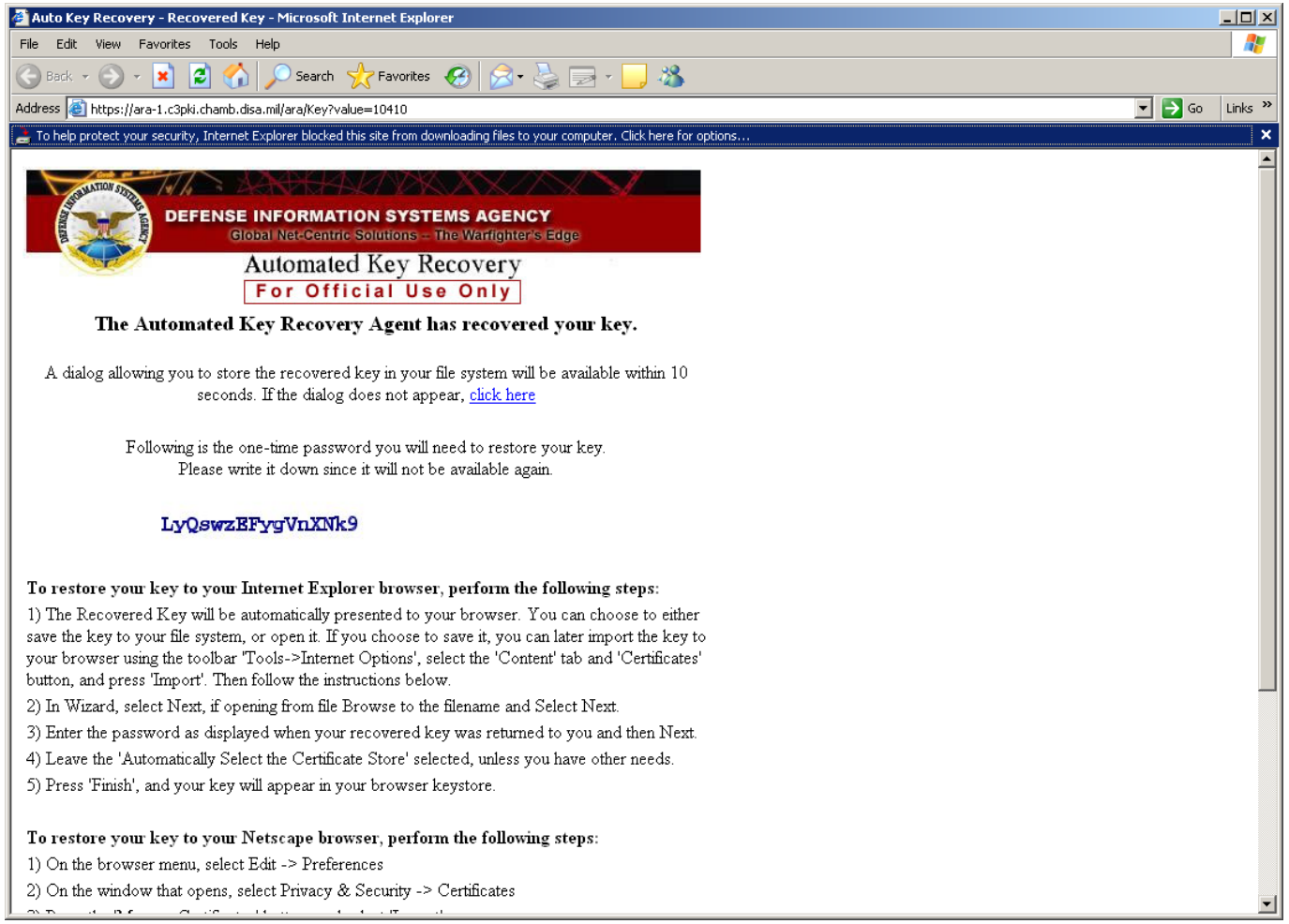
Installing the Certificate


Open
File Download
Do you want to open or save this file?
Name: ara_recovered_key.p12
Type: Personal Information Exchange, 2.34 KB
From: ara-1.c3pki.chamb.disa.mil
Open
Save
Cancel
Always ask before opening this type of file
While files from the Internet can be useful, some files can potentially harm your computer. If you do not trust the source, do not open or save this file. What's the risk?

Click "Open"

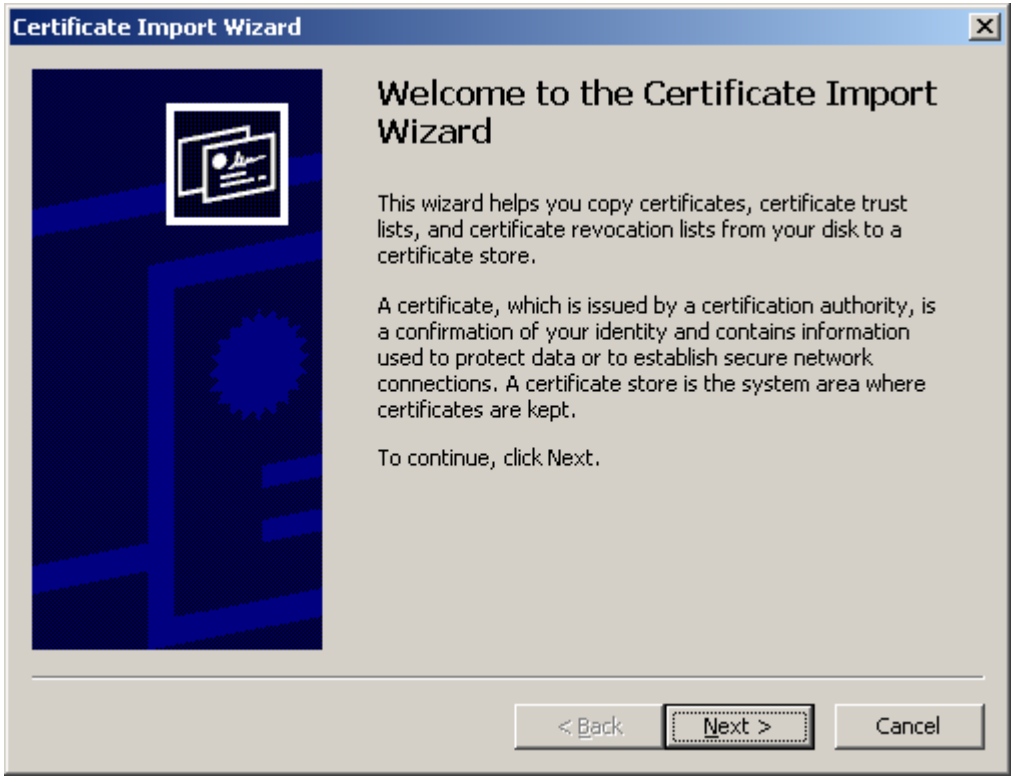
Depending on your browsers settings, you may see the next slide

File Download Blocked Warning


Auto Key Recovery - Recovered Key - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address https://ara-1.c3pki.chamb.disa.mil/ara/Key?value=10410
Go Links
To help protect your security, Internet Explorer blocked this site from downloading files to your computer. Click here for options...
DEFENSE INFORMATION SYSTEMS AGENCY
Global Net-Centric Solutions -- The Warfighter's Edge
Automated Key Recovery
For Official Use Only
The Automated Key Recovery Agent has recovered your key.
A dialog allowing you to store the recovered key in your file system will be available within 10 seconds. If the dialog does not appear, click here
Following is the one-time password you will need to restore your key.
Please write it down since it will not be available again.
LyQswzEFygVnXNk9
To restore your key to your Internet Explorer browser, perform the following steps:
1) The Recovered Key will be automatically presented to your browser. You can choose to either save the key to your file system, or open it. If you choose to save it, you can later import the key to your browser using the toolbar 'Tools->Internet Options', select the 'Content' tab and 'Certificates' button, and press 'Import'. Then follow the instructions below.
2) In Wizard, select Next, if opening from file Browse to the filename and Select Next.
3) Enter the password as displayed when your recovered key was returned to you and then Next.
4) Leave the 'Automatically Select the Certificate Store' selected, unless you have other needs.
5) Press 'Finish', and your key will appear in your browser keystore.
To restore your key to your Netscape browser, perform the following steps:
1) On the browser menu, select Edit -> Preferences
2) On the window that opens, select Privacy & Security -> Certificates

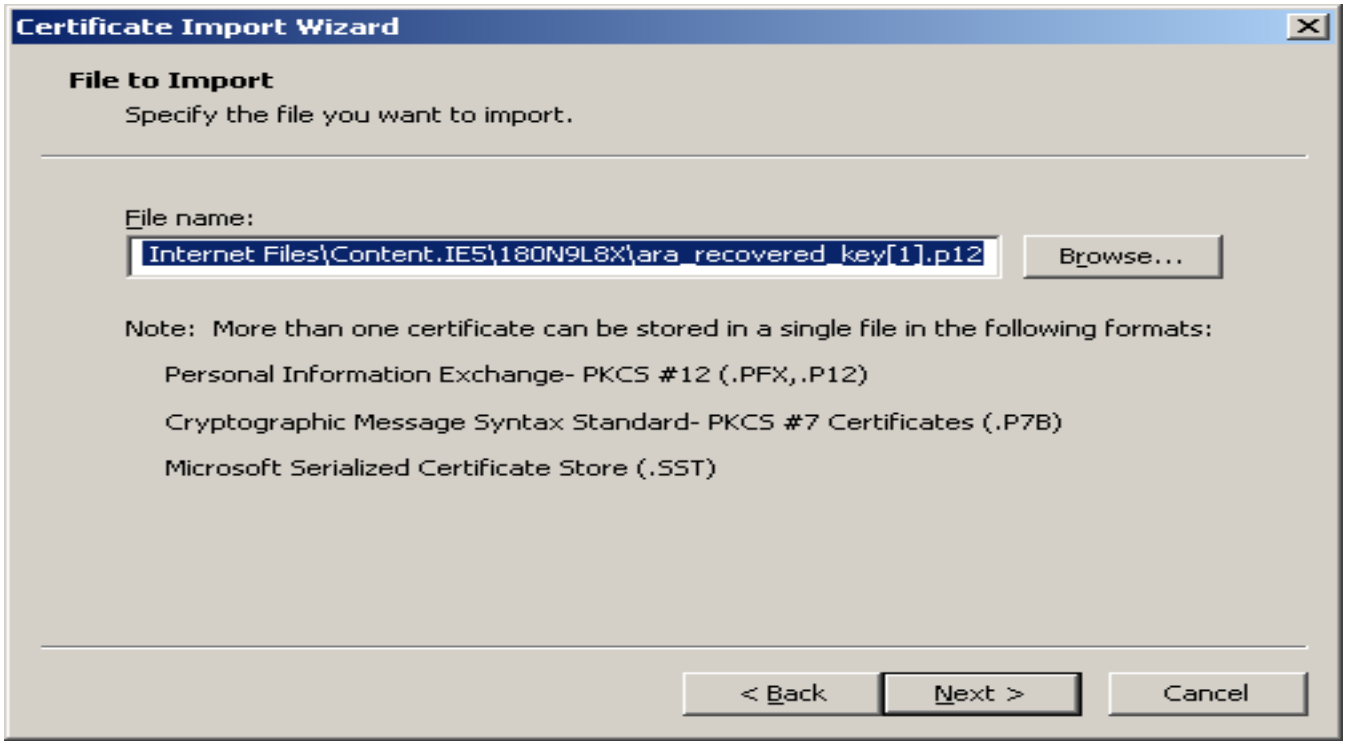
If you get this window, right-click the message and select “download file”.

Installing the Certificate (Cont'd)


Certificate Import Wizard
Welcome to the Certificate Import Wizard
This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.
A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.
To continue, click Next.
< Back
Next >
Cancel

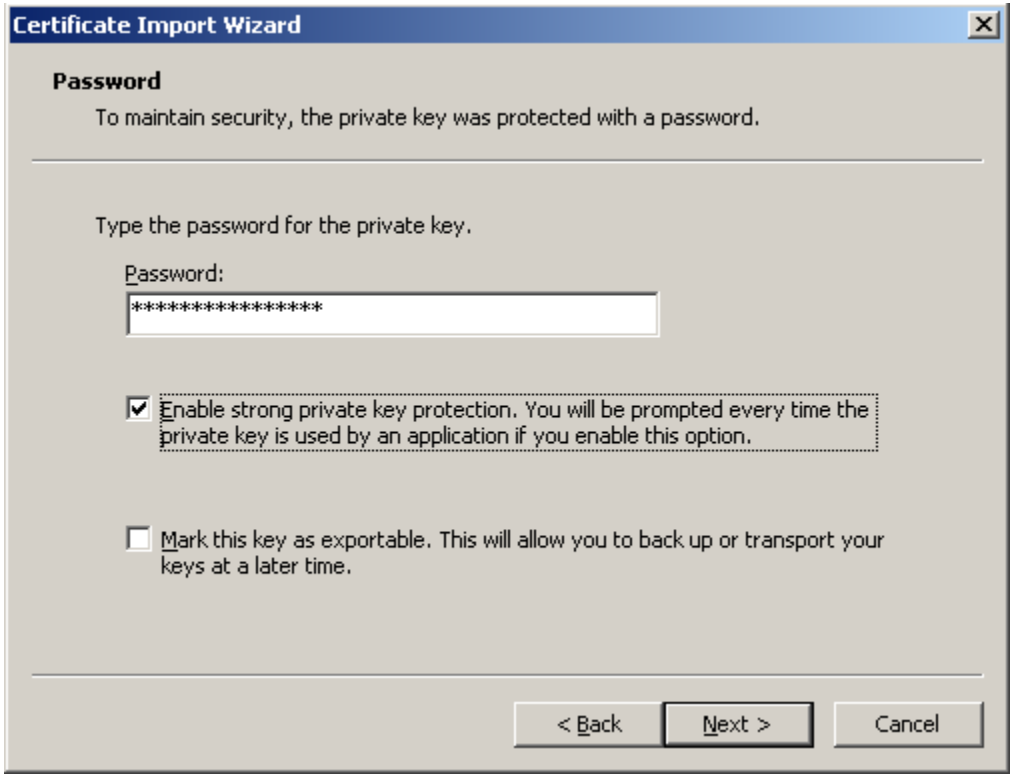
Click "Next".

Installing the Certificate (Cont'd)


Certificate Import Wizard
File to Import
Specify the file you want to import.
File name:
Internet Files\Content.IE5\180N9L8X\ara_recovered_key[1].p12
Browse...
Note: More than one certificate can be stored in a single file in the following formats:
Personal Information Exchange- PKCS #12 (.PFX,.P12)
Cryptographic Message Syntax Standard- PKCS #7 Certificates (.P7B)
Microsoft Serialized Certificate Store (.SST)
< Back
Next >
Cancel

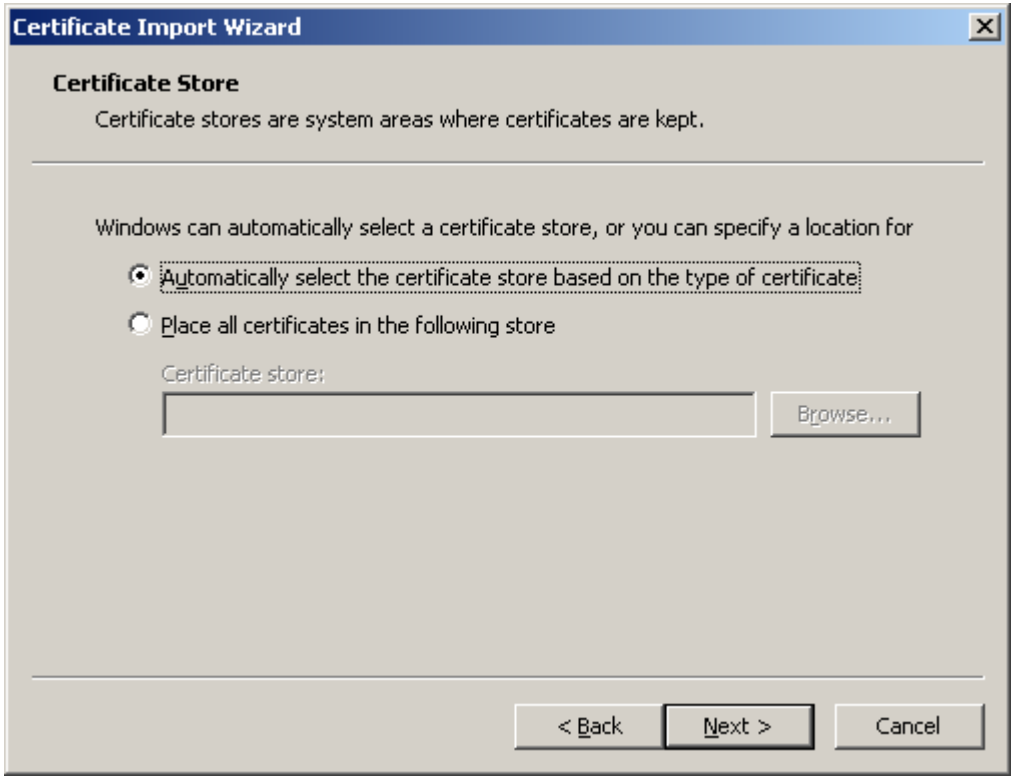
Accept the defaults; Click "Next".

Installing the Certificate (Cont'd)


Certificate Import Wizard
Password
To maintain security, the private key was protected with a password.
Type the password for the private key.
Password:
****
Enable strong private key protection. You will be prompted every time the private key is used by an application if you enable this option.
Mark this key as exportable. This will allow you to back up or transport your keys at a later time.
< Back
Next >
Cancel

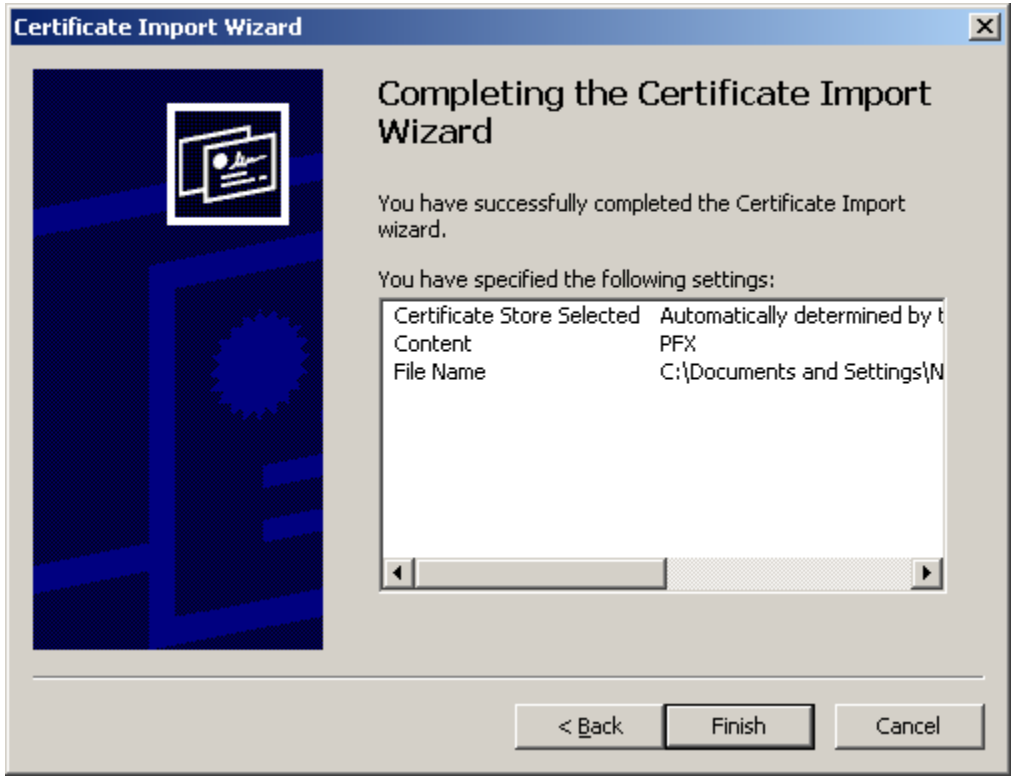
Leave the check blocks unchecked, enter your Password, and click "Next".

Installing the Certificate (Cont'd)


Certificate Import Wizard
Certificate Store
Certificate stores are system areas where certificates are kept.
Windows can automatically select a certificate store, or you can specify a location for
Automatically select the certificate store based on the type of certificate
Place all certificates in the following store
Certificate store:
Browse...
< Back
Next >
Cancel

Accept defaults – should be as shown above and click "Next".

Installing the Certificate (Cont'd)



Click "Finish".

Installing the Certificate (Cont'd)

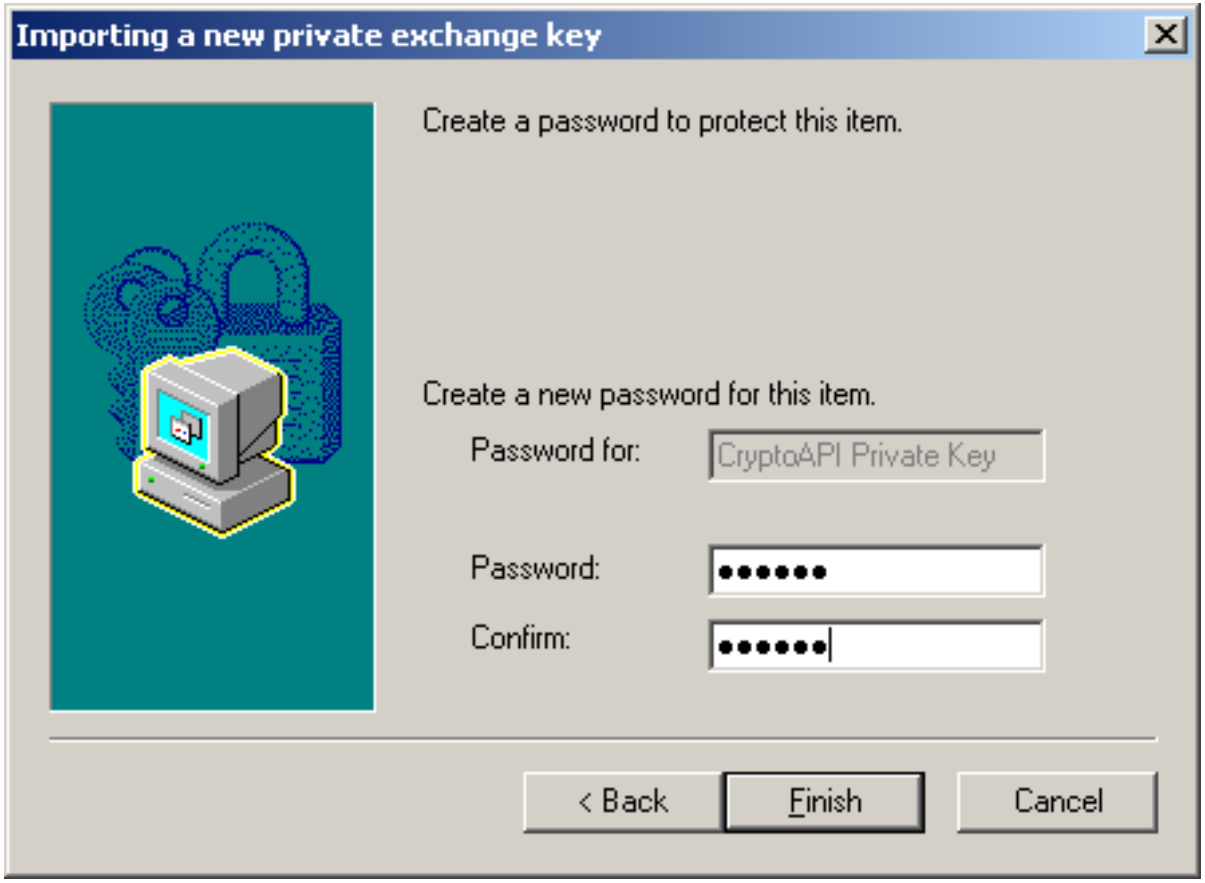
Click "Set Security Level"

Installing the Certificate (Cont'd)

Importing a new private exchange key
Choose a security level appropriate for this item.
High
Request my permission with a password when this item is to be used.
Medium
Request my permission when this item is to be used.
< Back
Next >
Cancel

Select "High" and "Next"

Installing the Certificate (Cont'd)



Enter Your CAC PIN as a Password and Click "Finish"
Note: Vista requires a 14 character password for this step

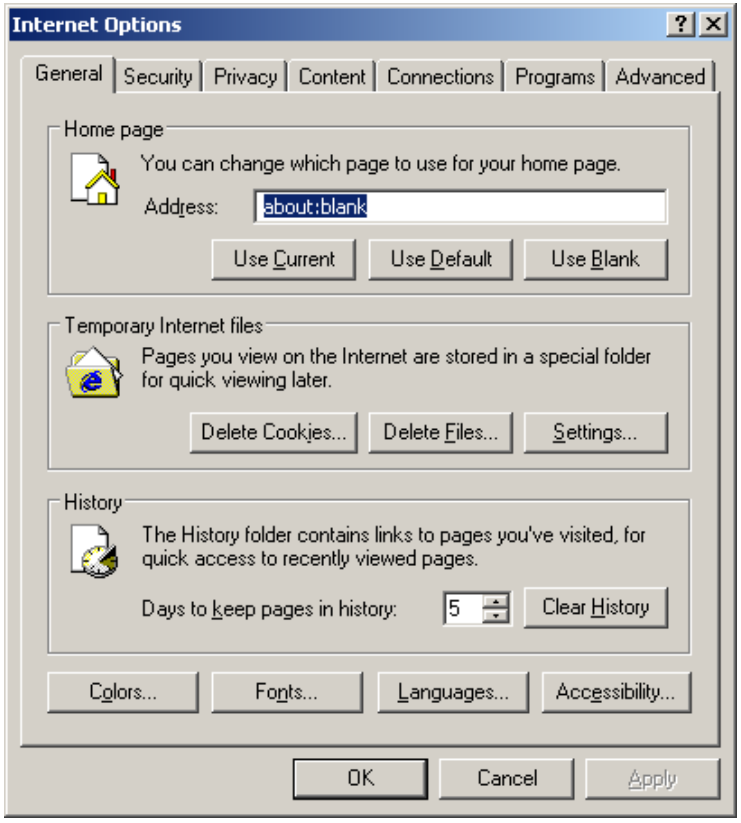
Installing the Certificate (Cont'd)

Click "OK"

Installing the Certificate (Cont’d)

Click “OK”.

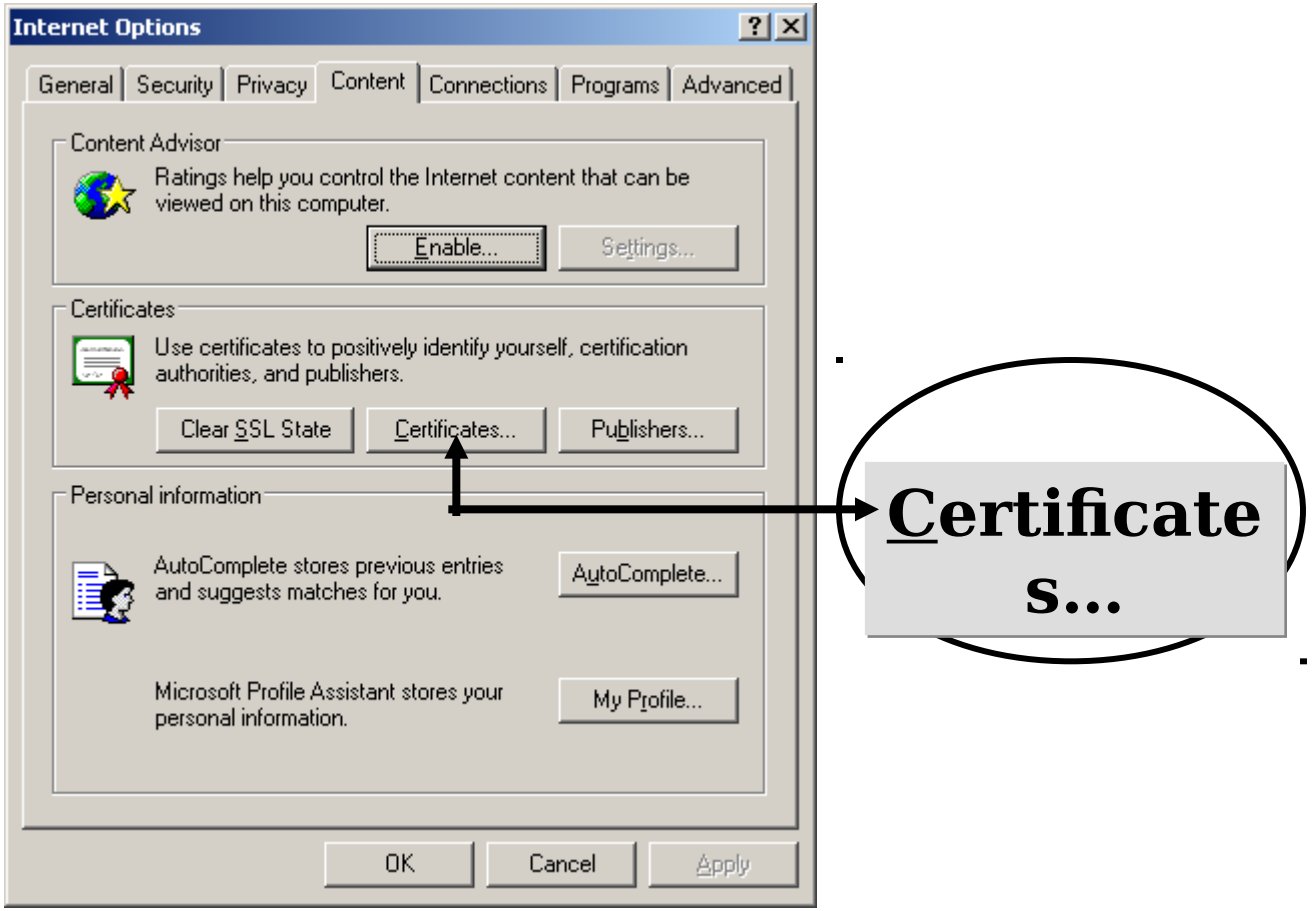
Verifying the Download



You can verify the successful download by performing the following;

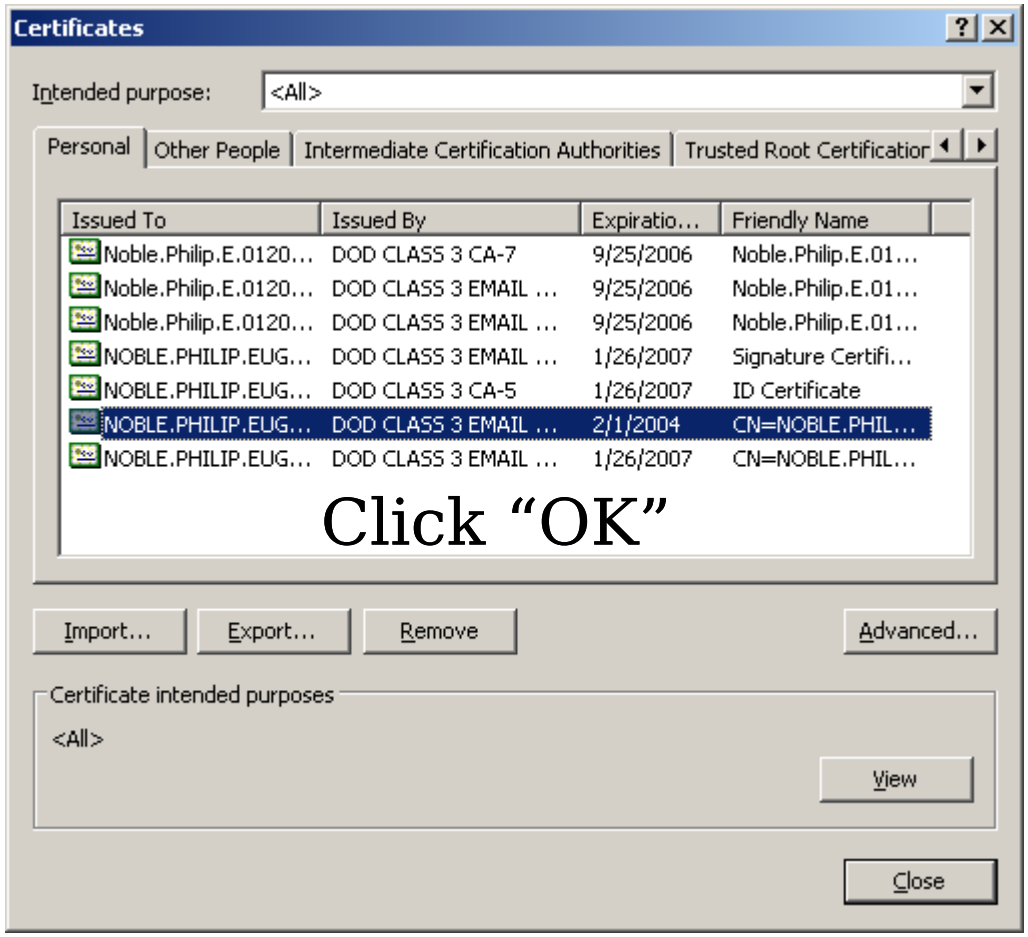
Launch Internet Explorer, select “Tools” from the menu, and then “Internet Options”.

Verifying the Download (Cont'd)



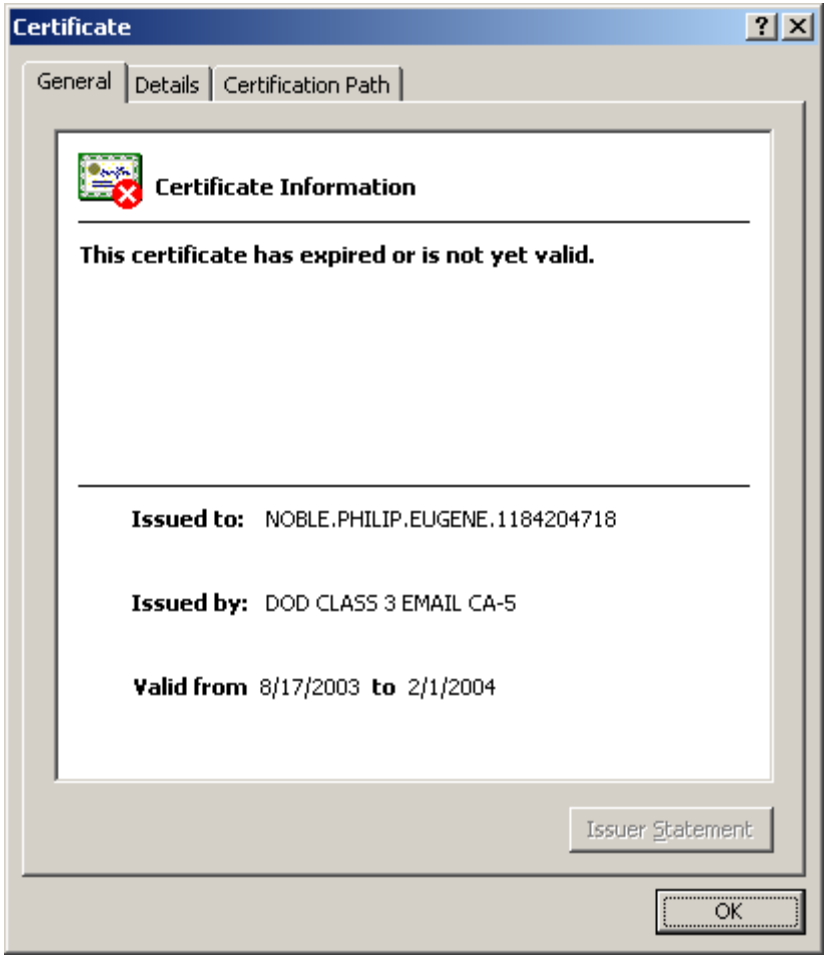
Click the "Content" tab; then click "Certificates".

Verifying the Download (Cont'd)



Select the "Personal" tab; you will see a list of your currently registered certificates, including the recovered new key certificate that starts with "**CN**"

Verifying the Download (Cont'd)



Double-click on the certificate and you can view the specifics of your recovered key (or other current keys) as illustrated above.

Success

Close the open window, you may now use the recovered key to access your encrypted email.

Last Step: Delete the .P12 file from you computer as this is a security vulnerability and will be detected in a Qtip Scan

Double-click on the certificate and you can view the specifics of your recovered key (or other current keys) as illustrated above.

Recovery Notification Example

A user has attempted to recover a key using the Automated Key Recovery Agent. The ID Certificate used for Authentication was: CN=NOBLE.PHILIP.EUGENE.1184204718,OU=USA,OU=PKI,OU=DOD,O=U.S. GOVERNMENT,C=US, Serial: 0x0B5643, Issuer: DOD CLASS 3 CA-5. The key that was recovered was: CN=NOBLE.PHILIP.EUGENE.1184204718,OU=USA,OU=PKI,OU=DOD,O=U.S. GOVERNMENT,C=US, Serial: 0x0C8747, Issuer: DOD CLASS 3 EMAIL CA-3.

If you did not perform this operation, please contact your local key recovery agent and ask that they check the logs for the key recovery at Fri Jul 01 16:48:12 GMT 2005 with session ID 1.c3pki.chamb.disa.mil-23f%3A42c57335%3A68e46e9395fb9727.

You should receive an email from PKI_ChambersburgProcessingElement@csd.disa.mil with a subject “ALERT! Key Recovery Attempt Using Automated Key Recovery Agent” similar to the above

Recovery Notification example notifying you of your recovery action.